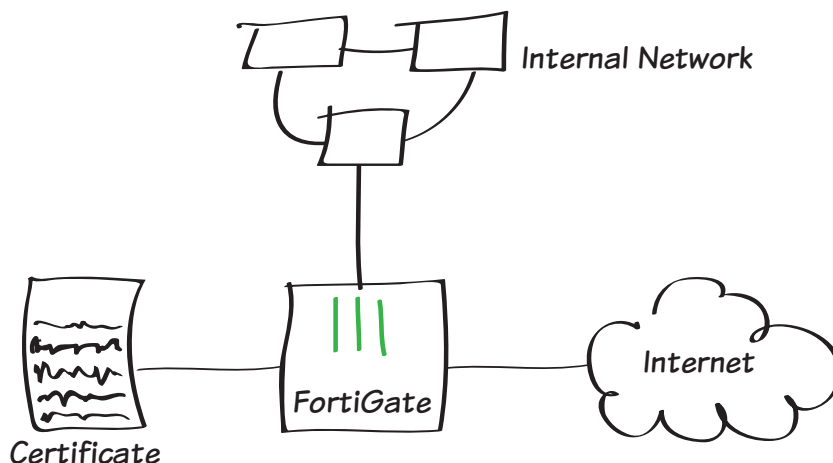


Using a custom certificate for SSL inspection

This recipe shows how use a FortiGate unit to generate a custom certificate signing request and to get this certificate signed by an enterprise root Certificate Authority (CA). This recipe also shows how to import the CA-signed certificate back into your FortiGate and how to add the certificate to an SSL inspection profile.

A certificate with *CA=TRUE* and/or *KeyUsage=CertSign* present in the metadata is necessary to perform deep inspection. By importing a custom certificate from a recognized third-party CA, you create a chain of trust that does not exist when the FortiGate's default certificate is used. This allows network users to trust the FortiGate as a CA in its own right.

1. Generating a certificate signing request (CSR)
2. Importing a signed server certificate from an enterprise root CA
3. Creating an SSL inspection profile
4. Configuring a firewall policy
5. Results



1. Generating a certificate signing request (CSR)

Go to **System > Certificates > Local Certificates** and select **Generate**.

In the **Generate Certificate Signing Request** page, fill out the required fields. You can enter a maximum of five **Organization Units**.

You may enter **Subject Alternative Names** for which the certificate is valid. Separate the names using commas.



To ensure PKCS12 compatibility, do not include spaces in the certificate name.

Certificate Name	<input type="text" value="MyCert"/>
Subject Information	
ID Type	<input type="text" value="Host IP"/>
IP	<input type="text" value="192.168.1.99"/>
Optional Information	
Organization Unit	<input type="text" value="Tech"/>
Organization	<input type="text" value="Fortinet"/>
Locality(City)	<input type="text" value="Ottawa"/>
State/Province	<input type="text" value="Ontario"/>
Country/Region	<input type="text" value="CANADA (CA)"/>
E-mail	<input type="text" value="tmanager@fortinet.com"/>
Subject Alternative Name	<input type="text" value="email:myemail@email.com"/>
Key Type	
	<input type="text" value="RSA"/>
Key Size	
	<input type="text" value="2048 Bit"/>
Enrollment Method	
<input checked="" type="radio"/> File Based <input type="radio"/> Online SCEP	

Go to **System > Certificates > Local Certificates** to view the certificate list. The status of the CSR created will be listed as **Pending**. Select the certificate and click **Download**.

This CSR will need to be submitted and signed by an enterprise root CA before it can be used. When submitting the file, ensure that the template for a **Subordinate Certification Authority** is used.

Delete Generate Import View Certificate Detail Download					
	Name			Status	Ref.
<input type="checkbox"/>	Fortinet_CA_SSLProxy	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU =		OK	2
<input type="checkbox"/>	Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU		OK	0
<input type="checkbox"/>	Fortinet_Factory2	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU		OK	0
<input type="checkbox"/>	Fortinet_Firmware	C = US, ST = California, L = Sunnyvale, O = Fortine		OK	1
<input type="checkbox"/>	Fortinet_SSLProxy	C = US, ST = California, L = Sunnyvale, O = Fortinet, C		OK	4
<input type="checkbox"/>	Fortinet_Wifi	OU = Domain Control Validat		OK	1
<input checked="" type="checkbox"/>	MyCert			PENDING	0

2. Importing a signed server certificate from an enterprise root CA

Once the CSR is signed by an enterprise root CA, you can import it into the FortiGate unit.

Go to **System > Certificates > Local Certificates** and click **Import**. From the **Type** drop down menu select **Local Certificate** and click **Choose File**.

Locate the certificate you wish to import, select it, and click **Open**.

The CA signed certificate will now appear on the **Local Certificates** list.



You can also use the FortiGate unit's default certificate. For information about using the default certificate, see [“Preventing security certificate warnings when using SSL full inspection”](#) on page 56.

Certificate Name	<input type="text" value="MyCert"/>
<hr/>	
Subject Information	
ID Type	<input type="text" value="Host IP"/>
IP	<input type="text" value="192.168.1.99"/>
<hr/>	
Optional Information	
Organization Unit	<input type="text" value="Tech"/>

Name	Date Modified
MyCert.cer	Jun 19, 2014, 9:56 AM

3. Creating an SSL inspection profile

To use your certificate in an SSL inspection profile go to **Policy & Objects > Policy > SSL/SSH Inspection**.

Create a new **SSL Inspection Profile**. In the **CA Certificate** drop down menu, select the certificate you imported. Set the **Inspection Method** to **Full SSL Inspection** and **Inspect All Ports**.

You may also need to select web categories and addresses to be exempt from SSL inspection. For more information on exemptions, see [“Preventing security certificate warnings when using SSL full inspection”](#) on page 56.

Name

My Inspection

Comments

Write a comment...

0/255

SSL Inspection Options

Enable SSL Inspection of

☒ Multiple Clients Connecting to Multiple Servers
☐ Protecting SSL Server

CA Certificate

MyCert

Inspection Method

☐ SSL Certificate Inspection ☒ Full SSL Inspection

☒ Inspect All Ports

ON

HTTPS

ON

SMTPS

ON

POP3S

ON

IMAPS

ON

FTPS



If the certificate does not appear in the list, verify that the template used to sign the certificate was for a CA and not simply for user or server identification.

4. Editing your Internet policy to use the new SSL inspection profile

Go to **Policy & Objects > Policy > IPv4** and edit the policy controlling Internet traffic.

Under **Security Profiles**, ensure that **SSL Inspection** and **Web Filter** are **On**. From the **SSL Inspection** dropdown menu, select your new profile. The **Web Filter** can remain as **default**.

Security Profiles	
<input type="button" value="OFF"/>	AntiVirus
<input checked="" type="button" value="ON"/>	Web Filter
<input type="button" value="OFF"/>	Application Control
<input type="button" value="OFF"/>	Email Filter
<input type="button" value="OFF"/>	DLP Sensor
Proxy Options	
<input checked="" type="button" value="ON"/>	SSL Inspection

default

default

default

default

default

default


default

My Inspection

5. Results

When visiting an HTTPS website such as <https://www.youtube.com/> a warning would normally appear if you are using a self-signed certificate.

If you have the correct type of certificate, signed by a recognized CA, warnings should no longer appear.



This Connection is Untrusted

You have asked Firefox to connect securely to **www.youtube.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

► Technical Details

▼ I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...

If you view the website's certificate information the **Issued By** section should contain the information of your custom certificate, indicating that the traffic is subject to deep inspection.

GeneralDetails

Could not verify this certificate because the issuer is not trusted.

Issued To

Common Name (CN)

*.google.com

Organization (O)

Google Inc

Organizational Unit (OU)

<Not Part Of Certificate>

Serial Number

34:10:F9:22:E2:0D:BF:E0:12:F6:54:53:CD:0D:BF:E0

Issued By

Common Name (CN)

fortinet.com

Organization (O)

Fortinet

Organizational Unit (OU)

Tech

Validity

Issued On

2014-06-04

Expires On

2014-09-01

Fingerprints

SHA1 Fingerprint

AE:7D:23:3D:73:69:F3:5B:20:6E:C6:DB:7B:48:73:64:2E:52:B4:38

MD5 Fingerprint

80:12:18:86:B8:E7:F0:0B:2F:DC:15:93:45:81:A0:62

Network users can now manually import the certificate into their trusted root CA certificate store (IE and Chrome) and/or into their browsers (Firefox).

Alternately, if the users are members of a Windows domain, the domain administrator can use a group policy to force them to trust the self-signed certificate the FortiGate is presenting.